CUPSA | ASPC

COMMUNIQUE

16-COM-002 Aug. 1, 2016

Release of Disaster Recovery Planning Guidance

The Credit Union Prudential Supervisors Association (CUPSA) has released Disaster Recovery Planning (DRP) Guidance, which outlines sound processes, policies and procedures related to recovery or continuation of infrastructure critical to an organization after a natural or human-related disaster.

This guidance was developed for use by credit unions and caisses populaires to increase awareness of DRP concepts, and to assist IT managers that are developing and implementing disaster recovery plans within their organizations.

Each CUPSA member jurisdiction may choose to apply the guidance in its current or amended form at its own discretion.

CUPSA will continue to monitor national and international research and guidance related to DRP in order to continuously enhance the risk management practices of Canadian credit unions and caisses populaires.

About CUPSA

The Credit Union Prudential Supervisors Association (CUPSA) is an interprovincial association composed of credit union prudential supervisors across Canada. CUPSA works toward maintaining a sound and sustainable credit union sector through joint actions. For more information, visit CUPSA's website at www.cupsa-aspc.ca.

Disaster Recovery Planning Guidance

Disaster Recovery Planning (DRP) refers to the processes, policies and procedures related to recovery or continuation of infrastructure critical to an organization after a natural or human-induced disaster.

For the purposes of this document, CUPSA will only be providing guidance on DRP around information technology as it applies to an organization's overall Business Continuity Planning (BCP) functions.

This guidance was developed for credit unions and caisses populaires to increase awareness of DRP concepts, and to assist IT managers that are developing and implementing disaster recovery plans within their organizations.

The areas noted in this document are intended to be scalable to the relative size, scope, complexity and risk profile of an institution. In addition to this paper, CUPSA encourages credit unions and caisses populaires to refer to guidance papers that have been created by other provincial regulatory bodies.

Disaster Recovery Planning (DRP) vs Business Continuity Planning (BCP)

DRP is a subset of BCP and should include planning for recovery of applications, data, hardware, communications (such as networking) and other IT infrastructure.

In contrast, BCP is an organization-wide program used to recover and restore business functionality after a disaster or extended disruption. This includes planning for non-IT related aspects such as personnel, facilities, crisis communication and reputation protection.

During BCP, organizations will determine the criticality and priority of business functions, and establish acceptable outage targets for these functions. The purpose of disaster recovery planning is to establish recovery processes and procedures to meet or exceed the objectives and targets required to maintain business functions identified during business continuity planning.

DRP Principles and Practices

Disaster recovery planning should flow from an organization's business continuity plan, and should focus in greater detail on IT infrastructure. It should provide for a quick and secure recovery of applications, data, hardware, communications (such as networking) and other IT infrastructure affected by a disaster scenario or incident. Disaster recovery planning could include the following components:

Technology Impact Assessment

An organization should conduct a technology impact assessment, which is an assessment and analysis of existing infrastructure required to support its critical functions. This could involve the following:

- Creating an inventory of existing IT infrastructure, including computing resources, databases, storage, security, network components, personnel and vendors (lists with key contact information);
- Performing an analysis of the failure of one or more components of the credit union's or caisse populaire's IT infrastructure and its impact on a critical function; and
- Setting recovery point objectives and recovery time objectives for applications and systems.

Disaster Recovery Plan (DR Plan)

Each organization should create a formal DR Plan, which can address the following elements:

- Key personnel contact information;
- Disaster recovery team – definition, roles and responsibilities;
- Supporting documentation – technology impact assessment documents, contracts, service-level agreements, supplier contact data, etc.;
- Restoration procedures, including:
    - Activation and notification procedures to signal when a disaster has been declared and how to keep information flowing;
    - Incident response procedures that address the initial stages of the disaster and the steps to be taken;
    - Damage assessment procedures that determine the damage experienced during the disaster, and focus restoration efforts;
    - Relocation and restoration procedures should work to recover critical IT applications and systems. Depending on the nature and extent of the disaster, decisions can be made to rebuild, restore from back-ups, or use other recovery methods.

DR Plan Testing

An organization's DR Plan should be tested regularly. Testing provides confidence and experience when responding to a real emergency. It is also a means of continually increasing the level of education and awareness of disaster situations and procedures. The results of any test should be summarized in a report to the board of directors.

Testing will help keep the DR Plan up-to-date, including contact information and recovery procedures. It can also ensure that estimates/timelines for recovery are realistic; that staff maintain their familiarity with the plan; and that the plan's procedures, alternate sites and infrastructure perform, as required.

Awareness and Training

An organization should strive to create DR Plans that are clear, concise, and understood by both management and staff. Management should promote awareness of disaster recovery and incident response practices within their organization. The DR team should have a reasonable level of training with respect to their responsibilities, and maintain this expertise on a regular basis.

DRP Roles and Responsibilities

CUPSA has identified key roles and responsibilities around DRP as follows:

Board of Directors

- Reviewing and approving disaster recovery policies which support the establishment, maintenance and testing of a DRP at the organization; and
- Reviewing DRP testing reports.

Senior Management

- Assigning appropriate resources and personnel to disaster recovery processes and efforts;
- Ensuring that an appropriate DRP is in place, regularly maintained, and effectively tested;
- Aligning the DRP and BCP initiatives and priorities to ensure that that they effectively support each other; and
- Providing reports on the management, maintenance and testing of an organization's DRP to the board of directors.

External/Internal Auditors

- Evaluating the DRP's design and effectiveness; and
- Confirming the appropriateness of the DRP in terms of safeguarding assets and contributing to the overall resiliency of the organization.

Third Party Service Providers

- Providing confirmation to credit unions or caisses populaires that hosted and outsourced DRP-related products, services or arrangements are in place and ready.

Regulators

- Providing guidance or sound business practices for DRPs at credit unions and caisses populaires;
- Assessing credit unions' and caisses populaires' DRPs to ensure that they are following industry best practices; and
- Ensuring credit unions and caisses populaires establish and implement action plans if assessments reveal that they failed to effectively adhere to sound business practices around disaster recovery planning.